

DERWENT TERMS AND CONDITIONS

Derwent shall not in any circumstances be liable or responsible for the completeness or accuracy of any Derwent translation and will not be liable for any direct, indirect, consequential or economic loss or loss of profit resulting directly or indirectly from the use of any translation by any customer.

Derwent Information Ltd. is part of The Thomson Corporation

Please visit our home page:

"WWW.DERWENT.CO.UK" (English)
"WWW.DERWENT.CO.JP" (Japanese)

MACHINE-ASSISTED TRANSLATION (MAT):

(19) 【発行国】
日本国特許庁 (JP)

(19)[ISSUING COUNTRY]
Japanese Patent Office (JP)

(12) 【公報種別】
公開特許公報 (A)

Laid-open (Kokai) patent application number
(A)

(11) 【公開番号】
特開平 6 - 309528

(11)[UNEXAMINED PATENT NUMBER]
Unexamined Japanese patent No. 6-309528

(43) 【公開日】
平成 6 年 (1994) 11 月 4
日

(43)[DATE OF FIRST PUBLICATION]
November 4th, Heisei 6 (1994)

(54) 【発明の名称】
IC カード

(54)[TITLE]
IC card

(51) 【国際特許分類第 5 版】
G06K 19/073
G06F 12/14 310 D
9293-5B

(51)[IPC]
G06K 19/073 G06F 12/14 310 D 9293-5B

【F I】
G06K 19/00 P 8623-5L

[FI]
G06K 19/00 P 8623-5L

【審査請求】
未請求

[EXAMINATION REQUEST]
UNREQUESTED

【請求項の数】 3

[NUMBER OF CLAIMS] 3

【出願形態】 O L

[Application form] O L

【全頁数】 4

[NUMBER OF PAGES] 4

(21) 【出願番号】
特願平 5 - 95793

(21)[APPLICATION NUMBER]
Japanese Patent Application No. 5-95793

(22) 【出願日】
平成 5 年 (1993) 4 月 22
日

(22)[DATE OF FILING]
April 22nd, Heisei 5 (1993)

(71)【出願人】

(71)[PATENTEE/ASSIGNEE]

【識別番号】

0 0 0 0 5 8 2 1

[ID CODE]

000005821

【氏名又は名称】

松下電器産業株式会社

Matsushita Electric Industrial Co., Ltd.

【住所又は居所】

大阪府門真市大字門真 1 0 0 6
番地

[ADDRESS]

(72)【発明者】

(72)[INVENTOR]

【氏名】 高木 伸哉

TAKAGI SHINYA

【住所又は居所】

大阪府門真市大字門真 1 0 0 6
番地 松下電器産業株式会社内

[ADDRESS]

(72)【発明者】

(72)[INVENTOR]

【氏名】 武藤 義弘

MUTO YOSHIHIRO

【住所又は居所】

大阪府門真市大字門真 1 0 0 6
番地 松下電器産業株式会社内

[ADDRESS]

(74)【代理人】

(74)[PATENT AGENT]

【弁理士】

[PATENT ATTORNEY]

【氏名又は名称】

小鍛治 明 (外 2 名)

KOKAJI AKIRA (et al.)

(57)【要約】

(57)[SUMMARY]

【目的】

セキュリティを確保しながらアクセス条件を変更することができるICカードを提供する。

[OBJECT]

The IC card which can change access conditions while ensuring security is provided.

【構成】

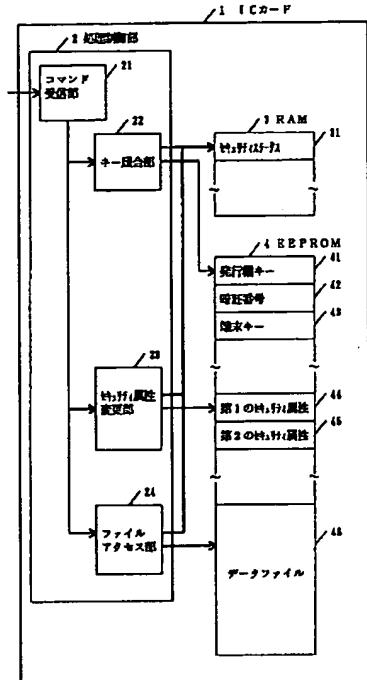
セキュリティステータス31はキーの照合結果を保持し、第1のセキュリティ属性44は、データファイル46を読み出すためのアクセス条件を格納する。外部より、このアクセス条件の変更指令があった時、セキュリティ属性変更部23は、セキュリティ属性44に格納されているアクセス条件が満たされているか否かをセキュリティステータス31により判定し、満たされている場合に限り、このアクセス条件の変更を行う。これ以後、データファイル46の読み出しは、変更されたアクセス条件の下で行われる。

[SUMMARY OF THE INVENTION]

The security status 31 maintains the comparison result of a key, and the first security attribute 44 stores the access conditions for reading a data file 46.

From the exterior, when there is a modification command of this access condition, the security attribute modification part 23 judges whether the access conditions stored by the security attribute 44 are fulfilled by the security status 31. Only when satisfied, this access condition is changed.

Read-out of this or later and the data file 46 is performed under the changed access conditions.



1. IC card

2. Process control part

21. Command receiver section

22. Key comparison part

23. Security attribute storage part

24. File access part

31. Security status

41. Machine key

42. Password

43. Terminal key

44. 1st security attribute

45 2nd security attribute

46. Data file

【特許請求の範囲】

[CLAIMS]

【請求項 1】

[CLAIM 1]

メモリと、前記メモリに対するアクセスを許可するアクセス条件を格納するセキュリティ属性記憶部と、外部からの指示により前記アクセス条件を更新する更新手段と、前記更新手段による前記アクセス条件の更新を許可または禁止する制御手段とを備えた I C カード。

【請求項 2】

制御手段は、セキュリティ属性記憶部に格納されているアクセス条件が満たされている場合に限り、前記アクセス条件の更新を許可することを特徴とする請求項 1 記載の I C カード。

【請求項 3】

外部からのアクセスの種類に対応した複数のセキュリティ属性記憶部を有し、制御手段は、前記複数のセキュリティ属性記憶部に格納されているアクセス条件が満たされている場合に限り、前記アクセス条件の更新を許可することを特徴とする請求項 1 記載の I C カード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】

本発明はキーの照合情報を用いて内蔵されるファイルに対するアクセス制御を行う I C カードに関する。

【0002】

Memory and security attribute storage part which stores the access conditions performing the approval of the access with respect to the above-mentioned memory. Updating means update the above-mentioned access conditions with external directions. Control means perform updating of the above-mentioned access conditions by above-mentioned updating means an approval or prohibition. The IC card provided with the above.

[CLAIM 2]

Controls means perform the approval of the updating of the above-mentioned access conditions, only when the access conditions stored by that security attribute storage part are fulfilled.

An IC card of Claim 1 characterized by the above-mentioned.

[CLAIM 3]

It has several security attribute storage part corresponded in the variety of external access.

Control means performs the approval of the updating of the above-mentioned access conditions, only when the access conditions stored by these security attribute storage part are fulfilled.

An IC card of Claim 1 characterized by the above-mentioned.

[DETAILED DESCRIPTION OF INVENTION]

[0001]

[INDUSTRIAL APPLICATION]

This invention relates to the IC card which performs access control with respect to the file incorporated using comparison information on a key.

[0002]

【従来の技術】

I CカードはC P U等の処理制御手段を有しているため、I Cカードに内蔵されるファイルごとに、そのファイルをアクセスするに先立って照合が必要となるキーに関する情報を設定し、これによってファイルに対するアクセス制御を行うことができる。このキーに関する情報をアクセス条件と呼ぶ。

[0003]

従来のI Cカードは、古くはデータメモリとしてE P R O Mを使用していたため、このアクセス条件は固定であった。また、近年になってデータメモリとしてE E P R O Mが使用されるようになっても、セキュリティの観点からアクセス条件は固定であった。

[0004]**【発明が解決しようとする課題】**

このような従来の構成では、I Cカードシステムの運用上、アクセス条件を変更したい状況が発生した場合、これに対応することができなかった。また、例えば、あるファイルのアクセス条件として、I Cカード所持者の暗証番号を設定している場合（すなわち、そのファイルをアクセスするためには、その前にI Cカード所持者の暗証番号の照合が必要であると設定している場合）、I Cカード所持者は必

[PRIOR ART]

Since the IC card has process control means, such as CPU, it precedes accessing that file for every file incorporated by the IC card, and sets up information about the key for which comparison is needed.

This can perform access control with respect to a file.

Information about this key is called access conditions.

[0003]

Since the conventional IC card was using E PROM as a data memory in the old days, this access condition was fixation.

Moreover, even when recent years are and EEPROM came to be used as a data memory, the viewpoint of security to access conditions were fixation.

[0004]**[PROBLEM ADDRESSED]**

With such conventional constitution, on the use of an IC card system, when the situation of wanting changing access conditions generated, it was not able to correspond in this.

Moreover, for example, as access conditions of a certain file, the case that an IC card possessor's password is set up (that is, when having set up if IC card possessor's password needs to be compared before it, in order to access that file). The IC card possessor had to input password.

It is convenient if the IC card possessor itself can switch over freely the essential/needlessness of password input.

However, this was not made in the conventional IC card.

ず暗証番号を入力しなければならなかった。暗証番号入力の要／不要を IC カード所持者自身が自由に切り替えることができれば便利であるが、従来の IC カードではこれができなかつた。

[0005]

本発明はこのような従来の問題点を解決するためのものであり、セキュリティを確保しながらアクセス条件を変更することができる IC カードを提供することを目的とする。

[0006]

【課題を解決するための手段】
上記の目的を達成するために本発明の IC カードは、メモリと、前記メモリに対するアクセスを許可するアクセス条件を格納するセキュリティ属性記憶部と、外部からの指示により前記アクセス条件を更新する更新手段と、前記更新手段による前記アクセス条件の更新を許可または禁止する制御手段とを備える。

[0007]**【作用】**

この構成により、アクセス条件の変更が可能となり、システムまたはユーザ側からの様々な要求に対応することが可能となる。また、あるアクセス条件を変更するためには、この変更前のアクセス条件を満たしている

[0005]

This invention is for solving such a conventional problem.

It aims at providing the IC card which can change access conditions while ensuring security.

[0006]**[SOLUTION OF THE INVENTION]**

In order that it attains the objective of an above, the IC card of this invention provides a memory, the security attribute storage part which store the access conditions performing the approval of the access with respect to the above-mentioned memory, updating means update the above-mentioned access conditions with external directions, and control means which perform the updating of the above-mentioned access conditions by above-mentioned updating means an approval or prohibition.

[0007]**[EFFECT]**

Modification of access conditions is possible by this constitution.

It can correspond in various demands from a system side or a user side.

Moreover, in order to change some access conditions, it is necessary to fulfill the access conditions before this modification.

Security is ensured.

ことが必要となり、セキュリティは確保される。

[0008]

【実施例】

(実施例1) 以下、本発明の第1の実施例について図面を参照しながら説明する。

[0009]

図1は本実施例のICカードの構成図であり、ICカード1は処理制御部2、RAM3と、電気的に書換えが可能なEEPROM4で構成される。処理制御部2はプログラムにより実現される処理ブロックで記述している。これらの処理内容については後述する。

[0010]

EEPROM4はデータファイル46を有している。このデータファイル46は、コマンド受信部21およびファイルアクセス部24を介して、外部からコマンドによりアクセスされる。

[0011]

第1のセキュリティ属性44には、データファイル46に対する第1のコマンド群(例えばファイルの読み出し)に対するアクセス条件が設定される。本実施例では、データファイル46の読み出し等の第1のコマンド群を実行するためには、「暗証番号42の照合が必要」と設定されているものとする。

[0008]

[Example]

(Example 1)) Hereafter, it explains, referring drawing about the first example of this invention.

[0009]

Fig. 1 is a block diagram of the IC card of this example.

IC card 1 consists of a process control part 2, and RAM 3 and EEPROM 4 which can be rewritten electrically.

Process control part 2, the process block realized by the program has described.

About these contents of a process, it mentions later.

[0010]

EEPROM 4 has the data file 46.

This data file 46 is accessed with a command from the exterior via the command receiver section 21 and the file access part 24.

[0011]

The access conditions with respect to the first command group (for example, read-out of a file) with respect to a data file 46 are set to the first security attribute 44.

In this example, in order to execute first command groups, such as read-out of a data file 46, it shall be set up that "comparison of the password 42 is necessity".

[0012]

同様に、第2のセキュリティ属性45には、データファイル46に対する第2のコマンド群（例えばファイルの書き込み）に対するアクセス条件が設定される。本実施例では、データファイル46の書き込み等の第2のコマンド群を実行するためには、「発行者キー41の照合が必要」と設定されているものとする。

[0013]

このようにセキュリティ属性44、45が設定されている場合、データファイル46の読み出し処理を伴うアプリケーションで本ICカードを使用する時、ICカード所持者は必ず暗証番号を入力しなければならない。多くのアプリケーションにおいて、データファイル46に書き込まれているデータの機密度に応じて、ICカード所持者が自由に暗証番号入力の要／不要の切り替えを行うことが必要となる。

[0014]

今、暗証番号42の入力を不要としたい時、ICカード所持者は、特定の場所に設置されている機器や携帯用端末機等（図示せず）で、暗証番号を解除するための所定の操作を行う。この所定の操作には、セキュリティを確保するため、暗証番号の入力が含まれる。

[0015]

端末機等は、まず入力された暗証番号をデータとしてキー照合

[0012]

Similarly, the access conditions with respect to the 2nd command group (for example, write of a file) with respect to a data file 46 are set to the 2nd security attribute 45.

In this example, in order to execute 2nd command groups, such as the write of a data file 46, it shall be set up that "comparison of the issue person key 41 is necessity".

[0013]

When the security attributes 44 and 45 are set up in this way, if using this IC card by the application accompanied by a read-out process of a data file 46, an IC card possessor has to input password.

In many applications, it is necessary to perform the switching of the essential/needlessness of password input of an IC card possessor free depending on the degree of secrecy of the data currently written in the data file 46.

[0014]

When he wants to make input of password 42 unnecessary now, the IC card possessor performs the predetermined operation for releasing password (not illustrated) with the apparatus. The portable terminal, etc. which are installed in the specific place.

Input of password is included in this predetermined operation in order to ensure security.

[0015]

A terminal etc. recognized the input password as a data and send the key comparison

コマンドを I C カード 1 に送信する。コマンド受信部 21 は、受信したコマンドがキー照合コマンドであることを解釈し、キー照合部 22 に制御を移す。

【0016】

キー照合部 22 は入力された暗証番号と、EEPROM4 に格納される暗証番号 42 とを比較し、一致した場合、「暗証番号が照合済み」という情報をセキュリティステータス 31 に書き込む。この情報は RAM3 内に書かれるため、I C カード 1 への電源が切れると消滅する一時的な情報である。

【0017】

次に前記の端末機等は、暗証番号の解除を指令するセキュリティ属性変更コマンドを I C カード 1 に送信する。

【0018】

コマンド受信部 21 は、受信したコマンドがセキュリティ属性変更コマンドであることを解釈し、セキュリティ属性変更部 23 に制御を移す。

【0019】

セキュリティを確保するため、セキュリティ属性変更部 23 は、第 1 のセキュリティ属性 44 に設定されている条件が満たされている場合に限り、この条件の変更が可能となるよう制御する。

【0020】

本実施例では、第 1 のセキュリ

command to IC card

The command receiver section 21 received interprets that it is a key comparison command.

A control is moved to the key comparison part 22.

[0016]

The key comparison part 22 compares the input password and password 42 stored by EEPROM4. When corresponding, the "password writes information of comparison which was completed" in the security status 31.

Since this information is written in RAM3, it is temporary information extinguished if the power supply to IC card 1 is cut.

[0017]

Next the above-mentioned terminal etc. transmits the security attribute modification command which commands releasing of password to IC card 1.

[0018]

The command receiver section 21 interprets that the received command is a security attribute modification command, and moves a control to the security attribute modification part 23.

[0019]

In order to ensure security, the security attribute modification part 23 is controlled to be able to perform modification of this condition, only when the conditions set as the first security attribute 44 are fulfilled.

[0020]

At this example, since it is set up that "comparison of the password 42 is necessity" to

ティ属性44には前述の通り、「暗証番号42の照合が必要」と設定されているため、本コマンドを実行するためには、暗証番号42が照合されていることが必要となる。すなわち、「暗証番号42の照合が必要」と設定されているものを更新するわけであるから、そのためには事前に暗証番号42を照合しておくことが必要条件となる。

[0021]

このように、あるセキュリティ属性を変更するためには、そのセキュリティ属性に設定されている変更前の条件を満たしていることを必要条件とすることにより、セキュリティは確保される。

[0022]

上記の制御を行うためにセキュリティ属性変更部23は、セキュリティステータス31に書かれている情報をチェックする。セキュリティステータス31には「暗証番号が照合済み」という情報が書き込まれているため、受信したセキュリティ属性変更コマンドの実行が許可される。セキュリティ属性変更部23は、「暗証番号42の照合が不要」という情報を第1のセキュリティ属性44に書き込む。この情報はEEPROM4内に記憶されるため、ICカード1に対する電源が切れても保持される。このようにして、以降、データファイル46の読み出し処理を伴うアプリケーションで本ICカードを使用する際、IC

the first security attribute 44 as above-mentioned. In order to execute this command, it is necessary to compare password 42.

That is, it updates that is set up "comparison of the password 42 is necessity". Therefore, it becomes a requisite for that to compare password 42 beforehand.

[0021]

Thus, in order to change a certain security attribute, security is ensured by making to fulfill the conditions before modification set as that security attribute into a requisite.

[0022]

In order to control an above, the security attributes modification part 23 checks information currently written to the security status 31.

Since information that "password comparison was completed" is written in the security status 31, the approval of the execution of a security attribute modification command which received is performed.

The security attribute modification part 23 writes information "comparison of password 42 is unnecessary" in the first security attribute 44.

Since it stores this information in EEPROM 4, Even when the power supply with respect to IC card 1 cuts, it maintains.

Thus, when using this IC card by the application accompanied by a read-out process of a data file 46 henceforth, it becomes unnecessary that an IC card possessor inputs password.

カード所持者は暗証番号を入力
することが不要となる。

[0023]

逆に、データファイル46を読み出すために暗証番号42の入力が必要となるよう再設定しなおす時も同様である。ただし、この場合は、第1のセキュリティ属性44に「暗証番号の照合は不要」と設定されているため、この変更処理を行うために暗証番号を入力する必要はない。

[0024]

このように本実施例によれば、あるセキュリティ属性を変更する場合、そのセキュリティ属性のアクセス条件が満足されていることが必要であるため、セキュリティを保持しながらセキュリティ属性を変更することが可能となる。

[0025]

(実施例2) 本発明の第2の実施例として、データファイル46への書き込み処理を発行機以外の機器（例えば商店のPOS端末など）で行えるようシステムを拡張する場合を考える。

[0026]

前述したように、データファイル46への書き込みに対するアクセス条件として、第2のセキュリティ属性45に「発行機キーの照合が必要」と設定されているため、各商店のPOS端末に発行機キーを登録する方法である。しかし、実際には発行機キーは、データファイル46への

[0023]

Conversely, it is similar when re-setting up so that input of password 42 may be needed in order to read a data file 46.

However, since it is set as the first security attribute 44 with "comparison of password is not necessary" in this case password does not need to be input in order to perform this modification process.

[0024]

According to this example in this way, when a certain security attribute is changed, it is required to satisfy the access conditions of that security attribute.

Therefore, a security attribute can be changed. While maintaining security.

[0025]

(Example 2) As the 2nd example of this invention, the case where a system is expanded so that apparatuses except for an issue machine (for example, POS terminal of a store etc.) can perform the write-in process to a data file 46 is considered.

[0026]

As mentioned above, it is set up that "comparison of the issue machine key is necessity" to the 2nd security attribute 45 as the access conditions with respect to the write to a data file 46. Therefore, it is the method of registering an issue machine key into POS terminal of each store.

However, an issue machine key is a key of the almighty which can also obtain authorities except for the write-in process to a data file 46, for example, rewriting of password etc., often in

書き込み処理以外の、例えば暗証番号の書換え等の権限をも得ることができる全能のキーであることが多い、このようなキーをPOS端末に置くことはセキュリティ上好ましくない。

[0027]

そこで、発行機キーとは別に端末キー43をICカード1およびPOS端末に設定し、この端末キー43を照合することにより、データファイル46への書き込みが可能となるようになることが望ましい。このために、第2のセキュリティ属性45は、「発行機キーの照合が必要」から「発行機キーまたは端末キーの照合が必要」へと更新することが必要となる。

[0028]

本実施例においても、第1の実施例と同様に、更新に先立って、変更前の条件である発行機キーの照合が必要となるため、セキュリティは確保される。

[0029]

以上の実施例では、あるセキュリティ属性を変更するために、そのセキュリティ属性に設定されている変更前の条件を満たしていることを必要条件とすることによってセキュリティを確保しているが、本発明はこれに限定されたものではない。

[0030]

例えば、あるセキュリティ属性を変更するために上位のキーの照合を必要とし、その条件をE

fact. It is not preferable to put such a key on POS terminal on security.

[0027]

Consequently, apart from an issue machine key, the terminal key 43 is set as IC card 1 and POS terminal.

By comparing this terminal key 43, it is preferable that the write to a data file 46 is made to be made.

For this reason, the 2nd security attribute 45, it is necessary to update "comparison of an issue machine key is necessity" to "comparison of an issue machine key or a terminal key is necessity".

[0028]

Also in this example, since updating is preceded and comparison of the issue machine key which is the condition before modification is needed as a first example, security is ensured.

[0029]

In the above example, security is ensured by making to fulfill the conditions before modification set as that security attribute, in order to change a certain security attribute into a requisite.

However, this invention is not a limited thing at this.

[0030]

For example, in order to change a certain security attribute, comparison of the key of a higher-order is needed.

It is fine even if it stores that condition in

E P R O M 4 内の別のフィール another field in EEPROM 4.
 ドに格納するとしてもよい。

【0031】

[0031]

【発明の効果】

以上のように本発明によれば、セキュリティ属性に格納されているアクセス条件が満たされている場合に限り、このアクセス条件の更新を許可する制御手段を有する構成とすることにより、セキュリティを確保しながらアクセス条件を変更することが可能となる。

[EFFECT OF THE INVENTION]

As mentioned above, according to this invention, as long as the access conditions stored by the security attribute are fulfilled. Control means which performs the approval of the updating of this access condition is had and made composition. Thereby, access conditions can be changed, ensuring security.

【図面の簡単な説明】

[BRIEF EXPLANATION OF DRAWINGS]

【図 1】

本発明の第 1 の実施例における I C カードの構成図

【符号の説明】

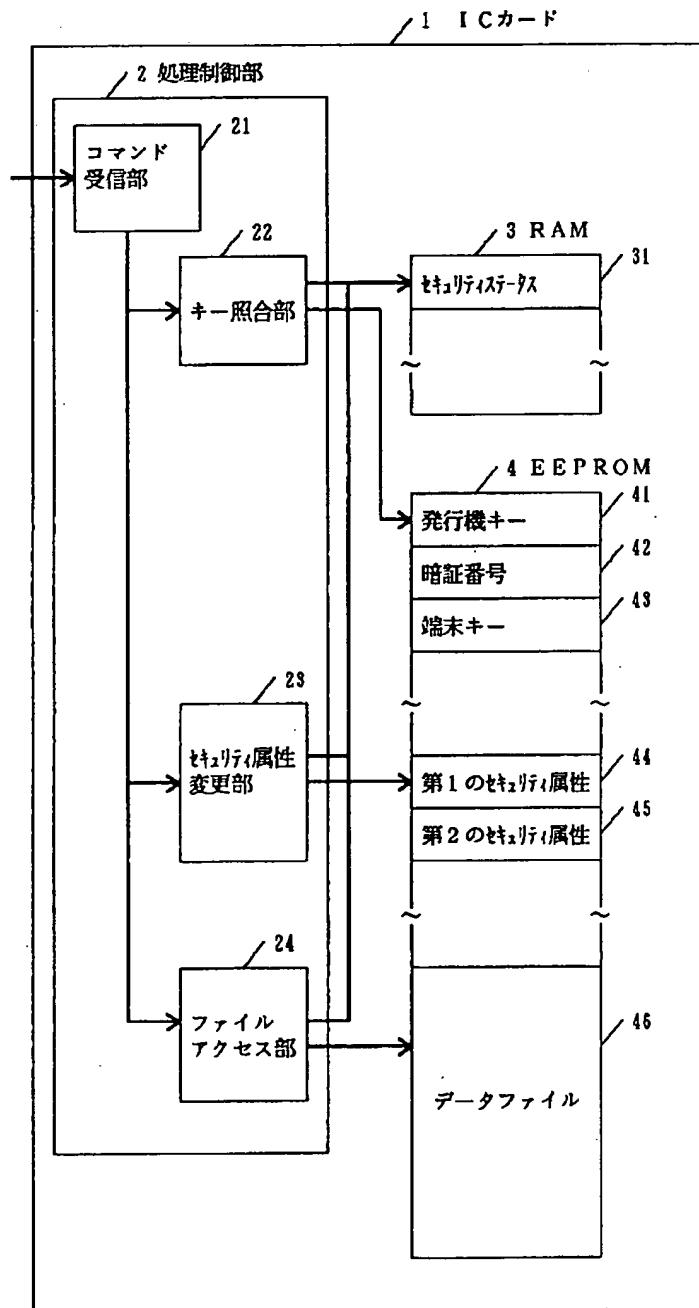
- 1 I C カード
- 2 処理制御部
- 3 R A M
- 4 E E P R O M
- 2 1 コマンド受信部
- 2 2 キー照合部
- 2 3 セキュリティ属性変更部
- 2 4 ファイルアクセス部
- 3 1 セキュリティステータス
- 4 1 発行機キー
- 4 2 暗証番号
- 4 3 端末キー
- 4 4 第 1 のセキュリティ属性
- 4 5 第 2 のセキュリティ属性
- 4 6 データファイル

[EXPLANATION OF DRAWING]

- 1 I C card
- 2 Process control part
- 3 RAM
- 4 EEPROM
- 21 Command receiver section
- 22 Key comparison part
- 23 Security attribute modification part
- 24 File access part
- 31 Security status
- 41 Issue machine key
- 42 Password
- 43 Terminal key
- 44 First security attribute
- 45 2nd security attribute
- 46 Data file

【図 1】

[FIGURE 1]



3. IC card

4. Process control part

- 21. Command receiver section
- 22. Key comparison part
- 23. Security attribute storage part
- 24. File access part

- 31. Security status

- 41. Machine key
- 42. Password
- 43. Terminal key
- 44. 1st security attribute
- 45 2nd security attribute
- 46. Data file

PTO 2002-2677

S.T.I.C. Translations Branch

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-309528

(43)公開日 平成6年(1994)11月4日

(51)Int.Cl.⁵
G 0 6 K 19/073
G 0 6 F 12/14

識別記号 庁内整理番号
3 1 0 D 9293-5B
8623-5L

F I
G 0 6 K 19/ 00

技術表示箇所
P

審査請求 未請求 請求項の数 3 O L (全 4 頁)

(21)出願番号

特願平5-95793

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(22)出願日 平成5年(1993)4月22日

(72)発明者 高木 伸哉

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 武藤 義弘

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

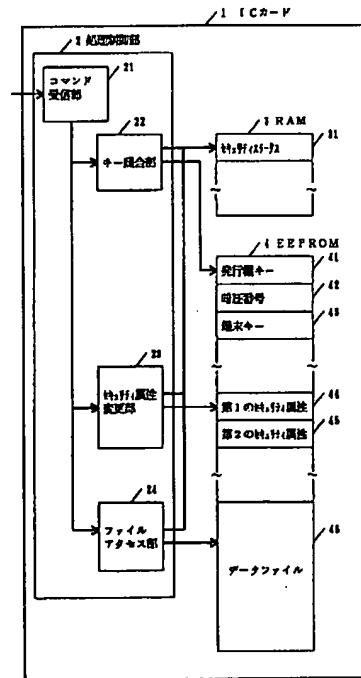
(74)代理人 弁理士 小銀治 明 (外2名)

(54)【発明の名称】 ICカード

(57)【要約】

【目的】 セキュリティを確保しながらアクセス条件を変更することができるICカードを提供する。

【構成】 セキュリティステータス31はキーの照合結果を保持し、第1のセキュリティ属性44は、データファイル46を読み出すためのアクセス条件を格納する。外部より、このアクセス条件の変更指令があった時、セキュリティ属性変更部23は、セキュリティ属性44に格納されているアクセス条件が満たされているか否かをセキュリティステータス31により判定し、満たされている場合に限り、このアクセス条件の変更を行う。これ以降、データファイル46の読み出しは、変更されたアクセス条件の下で行われる。



【特許請求の範囲】

【請求項1】メモリと、前記メモリに対するアクセスを許可するアクセス条件を格納するセキュリティ属性記憶部と、外部からの指示により前記アクセス条件を更新する更新手段と、前記更新手段による前記アクセス条件の更新を許可または禁止する制御手段とを備えたICカード。

【請求項2】制御手段は、セキュリティ属性記憶部に格納されているアクセス条件が満たされている場合に限り、前記アクセス条件の更新を許可することを特徴とする請求項1記載のICカード。

【請求項3】外部からのアクセスの種類に対応した複数のセキュリティ属性記憶部を有し、制御手段は、前記複数のセキュリティ属性記憶部に格納されているアクセス条件が満たされている場合に限り、前記アクセス条件の更新を許可することを特徴とする請求項1記載のICカード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はキーの照合情報を利用して内蔵されるファイルに対するアクセス制御を行うICカードに関する。

【0002】

【従来の技術】ICカードはCPU等の処理制御手段を有しているため、ICカードに内蔵されるファイルごとに、そのファイルをアクセスするに先立って照合が必要となるキーに関する情報を設定し、これによってファイルに対するアクセス制御を行うことができる。このキーに関する情報をアクセス条件と呼ぶ。

【0003】従来のICカードは、古くはデータメモリとしてEEPROMを使用していたため、このアクセス条件は固定であった。また、近年になってデータメモリとしてEEPROMが使用されるようになっても、セキュリティの観点からアクセス条件は固定であった。

【0004】

【発明が解決しようとする課題】このような従来の構成では、ICカードシステムの運用上、アクセス条件を変更したい状況が発生した場合、これに対応することができなかった。また、例えば、あるファイルのアクセス条件として、ICカード所持者の暗証番号を設定している場合（すなわち、そのファイルをアクセスするためには、その前にICカード所持者の暗証番号の照合が必要であると設定している場合）、ICカード所持者は必ず暗証番号を入力しなければならなかった。暗証番号入力の要／不要をICカード所持者自身が自由に切り替えることができれば便利であるが、従来のICカードではこれができなかった。

【0005】本発明はこのような従来の問題点を解決するためのものであり、セキュリティを確保しながらアクセス条件を変更することができるICカードを提供する

ことを目的とする。

【0006】

【課題を解決するための手段】上記の目的を達成するために本発明のICカードは、メモリと、前記メモリに対するアクセスを許可するアクセス条件を格納するセキュリティ属性記憶部と、外部からの指示により前記アクセス条件を更新する更新手段と、前記更新手段による前記アクセス条件の更新を許可または禁止する制御手段とを備える。

10 【0007】

【作用】この構成により、アクセス条件の変更が可能となり、システムまたはユーザ側からの様々な要求に対応することが可能となる。また、あるアクセス条件を変更するためには、この変更前のアクセス条件を満たしていることが必要となり、セキュリティは確保される。

【0008】

【実施例】

（実施例1）以下、本発明の第1の実施例について図面を参照しながら説明する。

20 【0009】図1は本実施例のICカードの構成図であり、ICカード1は処理制御部2、RAM3と、電気的に書換が可能なEEPROM4で構成される。処理制御部2はプログラムにより実現される処理ブロックで記述している。これらの処理内容については後述する。

【0010】EEPROM4はデータファイル46を有している。このデータファイル46は、コマンド受信部21およびファイルアクセス部24を介して、外部からコマンドによりアクセスされる。

【0011】第1のセキュリティ属性44には、データファイル46に対する第1のコマンド群（例えばファイルの読み出し）に対するアクセス条件が設定される。本実施例では、データファイル46の読み出し等の第1のコマンド群を実行するためには、「暗証番号42の照合が必要」と設定されているものとする。

【0012】同様に、第2のセキュリティ属性45には、データファイル46に対する第2のコマンド群（例えばファイルの書き込み）に対するアクセス条件が設定される。本実施例では、データファイル46の書き込み等の第2のコマンド群を実行するためには、「発行者キー441の照合が必要」と設定されているものとする。

【0013】このようにセキュリティ属性44、45が設定されている場合、データファイル46の読み出し処理を伴うアプリケーションで本ICカードを使用する時、ICカード所持者は必ず暗証番号を入力しなければならない。多くのアプリケーションにおいて、データファイル46に書き込まれているデータの機密度に応じて、ICカード所持者が自由に暗証番号入力の要／不要の切り替えを行ふことが必要となる。

【0014】今、暗証番号42の入力を不要としたい時、ICカード所持者は、特定の場所に設置されている

機器や携帯用端末機等（図示せず）で、暗証番号を解除するための所定の操作を行う。この所定の操作には、セキュリティを確保するため、暗証番号の入力が含まれる。

【0015】端末機等は、まず入力された暗証番号をデータとしてキー照合コマンドをICカード1に送信する。コマンド受信部21は、受信したコマンドがキー照合コマンドであることを解釈し、キー照合部22に制御を移す。

【0016】キー照合部22は入力された暗証番号と、EEPROM4に格納される暗証番号42とを比較し、一致した場合、「暗証番号が照合済み」という情報をセキュリティステータス31に書き込む。この情報はRAM3内に書かれるため、ICカード1への電源が切れると消滅する一時的な情報である。

【0017】次に前記の端末機等は、暗証番号の解除を指令するセキュリティ属性変更コマンドをICカード1に送信する。

【0018】コマンド受信部21は、受信したコマンドがセキュリティ属性変更コマンドであることを解釈し、セキュリティ属性変更部23に制御を移す。

【0019】セキュリティを確保するため、セキュリティ属性変更部23は、第1のセキュリティ属性44に設定されている条件が満たされている場合に限り、この条件の変更が可能となるよう制御する。

【0020】本実施例では、第1のセキュリティ属性44には前述の通り、「暗証番号42の照合が必要」と設定されているため、本コマンドを実行するためには、暗証番号42が照合されていることが必要となる。すなわち、「暗証番号42の照合が必要」と設定されているものを更新するわけであるから、そのためには事前に暗証番号42を照合しておくことが必要条件となる。

【0021】このように、あるセキュリティ属性を変更するためには、そのセキュリティ属性に設定されている変更前の条件を満たしていることを必要条件とすることにより、セキュリティは確保される。

【0022】上記の制御を行うためにセキュリティ属性変更部23は、セキュリティステータス31に書かれている情報をチェックする。セキュリティステータス31には「暗証番号が照合済み」という情報が書き込まれているため、受信したセキュリティ属性変更コマンドの実行が許可される。セキュリティ属性変更部23は、「暗証番号42の照合が不要」という情報を第1のセキュリティ属性44に書き込む。この情報はEEPROM4内に記憶されるため、ICカード1に対する電源が切れても保持される。このようにして、以降、データファイル46の読み出し処理を伴うアプリケーションで本ICカードを使用する際、ICカード所持者は暗証番号を入力することが不要となる。

【0023】逆に、データファイル46を読み出すため

に暗証番号42の入力が必要となるよう再設定しなおす時も同様である。ただし、この場合は、第1のセキュリティ属性44に「暗証番号の照合は不要」と設定されているため、この変更処理を行うために暗証番号を入力する必要はない。

【0024】このように本実施例によれば、あるセキュリティ属性を変更する場合、そのセキュリティ属性のアクセス条件が満たされていることが必要であるため、セキュリティを保持しながらセキュリティ属性を変更することが可能となる。

【0025】（実施例2）本発明の第2の実施例として、データファイル46への書き込み処理を発行機以外の機器（例えば商店のPOS端末など）で行えるようシステムを拡張する場合を考える。

【0026】前述したように、データファイル46への書き込みに対するアクセス条件として、第2のセキュリティ属性45に「発行機キーの照合が必要」と設定されているため、各商店のPOS端末に発行機キーを登録する方法である。しかし、実際には発行機キーは、データファイル46への書き込み処理以外の、例えば暗証番号の書き換え等の権限を得ることができる全能のキーであることが多く、このようなキーをPOS端末に置くことはセキュリティ上好ましくない。

【0027】そこで、発行機キーとは別に端末キー43をICカード1およびPOS端末に設定し、この端末キー43を照合することにより、データファイル46への書き込みが可能となるようになることが望ましい。このために、第2のセキュリティ属性45は、「発行機キーの照合が必要」から「発行機キーまたは端末キーの照合が必要」へと更新することが必要となる。

【0028】本実施例においても、第1の実施例と同様に、更新に先立って、変更前の条件である発行機キーの照合が必要となるため、セキュリティは確保される。

【0029】以上の実施例では、あるセキュリティ属性を変更するために、そのセキュリティ属性に設定されている変更前の条件を満たしていることを必要条件とするこによってセキュリティを確保しているが、本発明はこれに限定されたものではない。

【0030】例えば、あるセキュリティ属性を変更するため上位のキーの照合を必要とし、その条件をEEPROM4内の別のフィールドに格納するとしてもよい。

【0031】

【発明の効果】以上のように本発明によれば、セキュリティ属性に格納されているアクセス条件が満たされている場合に限り、このアクセス条件の更新を許可する制御手段を有する構成とすることにより、セキュリティを確保しながらアクセス条件を変更することが可能となる。

【図面の簡単な説明】

【図1】本発明の第1の実施例におけるICカードの構成図

5

6

【符号の説明】

- 1 ICカード
 2 構成制御部
 3 RAM
 4 EEPROM
 21 コマンド受信部
 22 キー照合部
 23 セキュリティ属性変更部
 24 ファイルアクセス部

- 24 ファイルアクセス部
 31 セキュリティステータス
 41 発行機キー
 42 暗証番号
 43 端末キー
 44 第1のセキュリティ属性
 45 第2のセキュリティ属性
 46 データファイル

【図1】

